Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

February 13, 2024

Challenge yourself with our Employment Scams Quiz!

Cybersecurity theme of the week: **Internet of Things (IoT)**
✪ Check out our **Internet of Things Thought Paper** to learn more.

Wonder what you can do to use IoT devices securely?

All Users	Technical Users	Business Owners
Make sure your IoT devices are updated to the latest version of their respective software.	Segment and isolate IoT devices/objects based on their purpose/function, require that the IoT device is configured securely, support authenticating and changing default passwords and disable unnecessary features and functions.	Ensure there is a policy in place updated regularly for the organizational use of IoT technologies.

This past week's stories:

🍁 **Montreal duo launch free cybersecurity training platform**

🍁 **Human trafficking victim says he was forced to target Canadians in crypto investment scam**

🍁 **Data breach impacts Canadian foreign affairs department**

Revealed – key cybersecurity breaches of 2023

Chinese hackers spent up to 5 years in US networks: Cyber officials

✪ **No, 3 million electric toothbrushes were not used in a DDoS attack**

Rise of malicious black hat AI tools that shifts the nature of cyber warfare

2024 Cybersecurity trends: AI and what's next

Huge surge in hackers exploiting QR code for phishing attacks

Ransomware attack disrupts services in 18 Romanian hospitals

‘Ounce of prevention’: Nebraska lawmakers seek $11 million for cybersecurity upgrades

4 ways hackers use social engineering to bypass MFA

Ransomware payments hitting record high, exceed $1 billion

Montreal duo launch free cybersecurity training platform

A man who targeted Canadians for cryptocurrency investment scams is speaking out after escaping the Cambodian compound where he was forced to do it.

https://www.itworldcanada.com/article/montreal-duo-launch-free-cybersecurity-training-platform/558568

Click above link to read more.

Back to top

Human trafficking victim says he was forced to target Canadians in crypto investment scam

A man who targeted Canadians for cryptocurrency investment scams is speaking out after escaping the Cambodian compound where he was forced to do it.

https://www.cbc.ca/news/business/crypto-scam-human-trafficking-1.7105454

Click above link to read more.

Back to top

Data breach impacts Canadian foreign affairs department

Canada’s foreign affairs department is reeling from the impacts of a data breach that leaked the personal information of users and staff members.

Global Affairs Canada (GAC), the country’s foreign affairs department, activated its cyber incident response plan and launched an investigation after detecting a cyber intrusion by a malicious actor.

https://www.cpomagazine.com/cyber-security/data-breach-impacts-canadian-foreign-affairs-department/

Click above link to read more.

Back to top

Revealed – key cybersecurity breaches of 2023

Tokio Marine HCC International (TMHCCI) has unveiled its Top 10 Cyber Incidents of 2023 report highlighting the most critical cyber incidents of the year, evaluating their financial and reputational impacts amid escalating geopolitical tensions and a surge in cyber-criminal activities.

https://www.insurancebusinessmag.com/ca/news/cyber/revealed--key-cybersecurity-breaches-of-2023-475898.aspx

Click above link to read more.

Back to top

Chinese hackers spent up to 5 years in US networks: Cyber officials

Hackers from the People's Republic of China spent up to five years in U.S. networks as part of a cyber operation that targeted U.S. critical infrastructure, law enforcement and international agencies said earlier this week.

https://abcnews.go.com/Politics/chinese-hackers-spent-5-years-us-networks-cyber/story?id=107059211

Click above link to read more.

Back to top

New malware mimic as Visual Studio update to attack macOS users

A new backdoor written in Rust has been discovered to target macOS users with several interesting features. Moreover, there have been 3 variants of backdoor found masquerading under the name of Visual Studio Update.

https://cybersecuritynews.com/malware-visual-studio-macos/

Click above link to read more.

Back to top

✪ No, 3 million electric toothbrushes were not used in a DDoS attack

A widely reported story that 3 million electric toothbrushes were hacked with malware to conduct distributed denial of service (DDoS) attacks is likely a hypothetical scenario instead of an actual attack.

https://www.bleepingcomputer.com/news/security/no-3-million-electric-toothbrushes-were-not-used-in-a-ddos-attack/

Click above link to read more.

Back to top

Rise of malicious black hat AI tools that shifts the nature of cyber warfare

The rise of malicious versions of LLMs, like dark variants of ChatGPT, is escalating cyber warfare by enabling more sophisticated and automated attacks.

https://cybersecuritynews.com/rise-of-black-hat-ai-tools/

Click above link to read more.

Back to top

2024 Cybersecurity trends: AI and what's next

Last year was marked by the irrefutable surge of artificial intelligence. The rapid expansion of AI and similar technologies has outpaced the development of effective cybersecurity management strategies.

https://www.forbes.com/sites/forbestechcouncil/2024/02/12/2024-cybersecurity-trends-ai-and-whats-next/?sh=73ca470f4b6c

Click above link to read more.

Back to top

Huge surge in hackers exploiting QR code for phishing attacks

Phishing has been one of the primary methods threat actors use for impersonating individuals or brands with a sense of urgency that could result in private information being entered on a malicious URL.

https://gbhackers.com/hackers-qr-code-for-phishing-attacks/

Click above link to read more.

Back to top

Ransomware attack disrupts services in 18 Romanian hospitals

The Romanian Ministry of Health has confirmed that its critical system is down due to the ransomware attack, and authorities are working to restore it.

https://www.hackread.com/ransomware-attack-hit-services-romania-hospitals/

Click above link to read more.

Back to top

‘Ounce of prevention’: Nebraska lawmakers seek $11 million for cybersecurity upgrades

Every 14 seconds, a successful ransomware attack hits a new target, and the cost of cybercrime is expected to climb to an annual cost of $10.5 trillion worldwide by 2025.

https://nebraskaexaminer.com/2024/02/12/ounce-of-prevention-nebraska-lawmakers-seek-11-million-for-cybersecurity-upgrades/

Click above link to read more.

Back to top

---

4 ways hackers use social engineering to bypass MFA

When it comes to access security, one recommendation stands out above the rest: multi-factor authentication (MFA). With passwords alone being simple work for hackers, MFA provides an essential layer of protection against breaches. However, it's important to remember that MFA isn't foolproof. It can be bypassed, and it often is.

https://thehackernews.com/2024/02/4-ways-hackers-use-social-engineering.html

Click above link to read more.

Back to top

Ransomware payments hitting record high, exceed $1 billion

Chainalysis, a leading blockchain analysis firm, has recently released a report on ransomware payments revealing that they have skyrocketed to a whopping $1 billion in 2023.

https://thehackernews.com/2024/02/4-ways-hackers-use-social-engineering.html

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****
****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

British Columbia OCIO Office of the Chief Information Officer